CUSTOMER NO.: 24498
Serial No.: 10/602,754
Final Office Action Dated: October 10, 2007

PATENT
PU030107 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicants: Larry Cecil Brown, et al.

Examiner: Matthew E. Heneghan

Serial No: 10/602,754

Group Art Unit: 2134

Filed: June 24, 2003

Docket: PU030107

For: REMOTE ACCESS CONTROL FEATURE FOR LIMITING ACCESS TO CONFIGURATION FILE COMPONENTS

Mail Stop Appeal Brief-Patents
Hon. Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Applicants appeal the status of claims 1-19 as presented in response to the Office Action dated June 5, 2007, and finally rejected in the Office Action dated October 10, 2007, **pursuant to the Notice of Appeal filed on February 5, 2008** and submit this appeal brief.

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being faxed to the United States Patent & Trademark Office, fax # 571-273-8300. Mail Stop: Appeal Brief-Patents on:

4-3-08
Date

Fideliz Romero
Fideliz Romero

TABLE OF CONTENTS:

from accessing the designated service provider accessible information, claim 10 is patentable over McMullan.

D. Conclusion

8. CLAIMS APPENDIX

9. RELATED EVIDENCE APPENDIX

10. RELATING PROCEEDINGS APPENDIX

1. Real Party in Interest

The real party in interest is THOMSON LICENSING S.A., the assignee of the entire right title and interest in and to the subject application by virtue of an assignment recorded with the Patent Office on June 7, 2004 at reel/frame 014702/0315.

2. Related Appeals and Interferences

None.

3. Status of Claims

Claims 1-19 are pending. Claims 1-19 stand rejected and are under appeal.

A copy of the claims 1-19 is presented in Section 8 below.

4. Status of Amendments

An amendment under 37 CFR §1.111, sent to the PTO on August 3, 2007 in response to the non-final Office Action dated June 5, 2007, was entered. A response under 37 C.F.R. §1.116, sent to the PTO on December 7, 2007 in response to the final Office Action dated October 10, 2007, was also entered. No Responses/Amendments were filed subsequent to the above response sent on December 7, 2007.

5. Summary of Claimed Subject Matter

Claim 1 is directed to a security system for use in a distributed network (see, e.g., element 10, FIG. 1), comprising: a service provider (see, e.g., element 100, FIG. 1) selectively accessible via a network (see, e.g., element 101, FIG. 1) by a plurality of end users each having an access device for accessing the network (see, e.g., elements 102, FIG. 1) (see also, p. 3, lines 21-31); and a control mechanism disposed at a location of the service provider (see, e.g., element 90, FIG. 1) which accesses and modifies stored information on each access device of the end users to designate service provider-accessible portions of the information to prevent access thereof by the end users (see, e.g., p. 5, line 15-35) (see also, e.g., p. 4, line 27 to p. 5, line 6).

Claim 10 is directed to method for maintaining system security for a network service provider, comprising the steps of: providing a control mechanism for remotely accessing and modifying end user network access devices (see, e.g., p. 5, lines 15-21); remotely accessing and modifying the end user network devices to designate service provider-accessible information stored on the access devices (see, e.g., p. 5, lines 28-35); and preventing the end user from accessing the designated service provider-accessible information on the end user's access device (see, e.g., p. 6, lines 2-3) (see also, e.g., p. 4, line 27 to p. 5, line 6).

6. <u>Grounds of Rejection to be Reviewed on Appeal</u>

Claims 1-8, 10 and 12-19 stand rejected under 35 U.S.C. §102(b) as being anticipated by McMullan, Jr., et al. (U.S. Patent No. 5,654,746) (hereinafter 'McMullan'). In addition, claims 9 and 11 stand rejected under 35 U.S.C. §103(a) as being unpatentable over McMullan. The preceding rejections are presented for review in this Appeal.

Regarding the grouping of the claims, claims 2-9 stand or fall with claim 1 and claims 11-19 stand or fall with claim 10, due to their respective dependencies.

7. Argument

A. Introduction

In general, aspects of the present principles are directed to a method and system for maintaining the security of proprietary information while providing communications service to network access devices. According to one implementation of the present principles, a service provider may remotely access and modify a configuration file stored on a user's access device to designate portions of stored information to be "service-provider access only" (see, e.g., Specification, p. 5, lines 17-21; p. 4, line 27 to p. 5, line 6). This feature enables a service provider to prevent a user from accessing information that may compromise its internal service security standards (see, e.g., Specification, p. 3, line 28 to p. 4, line 2) (see also, Specification, p. 1, lines 18-25). Furthermore, the "service provider access only" designation advantageously enables the service provider to continue to access the information after it is so designated so that it may adequately provide network communications service to a user (see, e.g., Specification, p. 5, lines 1-3; p. 5, lines 32-35; 108, Fig. 2).

Claim 1 includes the feature of remotely designating service-provider accessible information that is stored on an access device to prevent a user from accessing the information. Similarly, claim 10 includes the features of remotely designating information stored on an access device and preventing a user from accessing the designated service provider accessible information. McMullan fails to disclose at least these features of claims 1 and 10. Thus, it is respectfully submitted that claims 1 and 10 are patentable over McMullan. As such, claims 1 and 10 are presented for review in this appeal.

B. Whether Claim 1 Is Anticipated Under 35 U.S.C. §102(b) by McMullan

B1. Claim 1 is patentable over McMullan, as McMullan fails to disclose the feature of remotely designating service-provider accessible information that is stored on an access device to prevent a user from accessing the information.

Because McMullan does not anticipate the feature of remotely designating service-provider accessible information that is stored on an access device to prevent a user from accessing the information, claim 1 is patentably distinct from McMullan. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single or prior art reference" (MPEP §2131, quoting Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)). The elements of claim 1 include, inter alia:

> a service provider selectively accessible via a network by a plurality of end users each having an access device for accessing the network; and
>
> a control mechanism disposed at a location of the service provider which accesses and modifies stored information on each access device of the end users to designate service provider-accessible portions of the information to prevent access thereof by the end users.

McMullan fails to describe at least the element of remotely designating service provider accessible portions of information that is stored on an access device to prevent access thereof by end users.

The system of McMullan is directed to delivering games to user's home game adapter through a network, such as a cable television network. In accordance with McMullan, the game delivery system downloads a game to a user's home game adapter after a user purchases time to play it. Upon expiration of the user-purchased time, the system of McMullan institutes a "reset" operation in the home game adapter to halt game play, wherein all registries are cleared, requiring a user to initiate a new download if she wishes play the game again (e.g., McMullan, column 7, lines 55-61; column 17, lines 2-4; column 12, lines 23-27). To manage user access to the downloaded games, the service provider accesses a pay to Pay-to-Play (PTP) table located in the home game adapter, which includes information concerning games that are authorized for download and the time purchased for game play (McMullan, column 11, lines 20-62). Other aspects of the McMullan system include configuration of a user device by a service provider to set a new adapter address, to set an adapter timeout setting routine, to disable a particular adapter for non-payment of subscriber bills and to perform other transactions (see, e.g., McMullan, column 17, lines 38-56).

However, none of the aspects described in McMullan anticipate the feature of remotely designating service provider-accessible portions of information that is stored on an access device to prevent access thereof by end users, as recited in claim 1. Firstly, while McMullan describes instituting a reset operation to delete a game upon expiration of purchased time, the reset operation fails to designate service provider accessible portions of information that is stored on an access device. Deletion of the game stored on the access device renders the game inaccessible to both a user and the service provider. Secondly, McMullan's description of configuring of a user device to set a new adapter address, to set a timeout setting routine and the like, do not constitute designation of stored information to prevent access thereof by the end users. Such actions do not designate any portions of information whatsoever to be inaccessible by a user. Thirdly, disabling a particular adapter for non-payment of bills fails to constitute designation of information, as recited in claim 1. As discussed above, designation of information in accordance with aspects of the present principles includes labeling information to be "service provider accessible only." Disabling a device does not in any way label information stored on the device.

Accordingly, McMullan fails to disclose at least the feature of remotely designating service provider-accessible portions of information that is stored on an access device to prevent access thereof by end users. Thus, claim 1 is patentable over McMullan. In addition, claims 2-9 are also patentable over McMullan due at least to their dependencies on claim 1. Therefore, withdrawal of the rejection of claims 1-9 is respectfully requested.

C. Whether Claim 10 Is Anticipated Under 35 U.S.C. §102(b) by McMullan

C1. Because McMullan fails to disclose the features of remotely accessing and modifying user-devices to designate information stored on the devices and preventing a user from accessing the designated service provider accessible information, claim 10 is patentable over McMullan.

Claim 10 is patentable over McMullan, as McMullan does not anticipate the features of remotely designating information stored on access devices and preventing a user from accessing the designated service provider accessible information. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single or prior art reference" (MPEP §2131, quoting Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)). The elements of claim 10 include, inter alia:

> providing a control mechanism for remotely accessing and modifying end user network access devices;
> remotely accessing and modifying the end user network devices to designate service provider-accessible information stored on the access devices; and
> preventing the end user from accessing the designated service provider-accessible information on the end user's access device.

As discussed above with respect to claim 1, McMullan fails to disclose at least the feature of remotely designating service provider accessible portions of information that is stored on an access device to prevent access thereof by end users. Accordingly, McMullan likewise does not disclose the features of remotely accessing and modifying user-devices to designate information stored on the devices and preventing a user from accessing the designated service provider accessible information, as recited in claim 10. Thus, claim 10 is patentable over McMullan for at least the reasons discussed above. Moreover, claims 11-19 are also patentable over McMullan due at least to their dependencies from claim 10. Withdrawal of the rejection of claims 10-19 is respectfully requested.

D. Conclusion

At least the above-identified limitations of the pending claims are not disclosed by the teachings of McMullan. Accordingly, it is respectfully requested that the Board reverse the rejection of claims 1-19.

Please charge the amount of $500.00, covering fee associated with the filing of the Appeal Brief, to **Thomson Licensing Inc., Deposit Account No. 07-0832**. In the event of any non-payment or improper payment of a required fee, the Commissioner is authorized to charge **Deposit Account No. 07-0832** as required to correct the error.

Respectfully submitted,

Dated: 4/3/08

BY:

Jeffrey D. Hale, Attorney for Applicants
Registration No.: 40,012
Telephone No.: (609) 734-6444

Thomson Licensing, LLC
2 Independence Way, Suite 200
Princeton, NJ 08540

8. CLAIMS APPENDIX

1. (Previously presented) A security system for use in a distributed network, comprising:

a service provider selectively accessible via a network by a plurality of end users each having an access device for accessing the network; and

a control mechanism disposed at a location of the service provider which accesses and modifies stored information on each access device of the end users to designate service provider-accessible portions of the information to prevent access thereof by the end users.

2. (Original) The system as recited in claim 1, wherein the stored information includes a configuration file for the access device.

3. (Original) The system as recited in claim 1, wherein service provider includes a security code for the designated portions to prevent access thereof by the end users.

4. (Original) The system as recited in claim 3, wherein the security code is associated with the designated portions at or before initializing the access devices.

5. (Original) The system as recited in claim 3, wherein the security code is associated with the designated portions after initializing the access devices.

6. (Original) The system as recited in claim 1, wherein service provider includes security levels for the information to prevent access thereof by the end users.

7. (Original) The system as recited in claim 6, wherein the security levels are associated with the designated portions at or before initializing the access devices.

8. (Original) The system as recited in claim 6, wherein the security levels are associated with the designated portions after initializing the access devices.

9. (Original) The system as recited in claim 1, wherein the control mechanism includes a software program for accessing and modifying the information of the access devices and designating portions thereof to prevent access by the end users.

10. (Previously presented) A method for maintaining system security for a network service provider, comprising the steps of:

providing a control mechanism for remotely accessing and modifying end user network access devices;

remotely accessing and modifying the end user network devices to designate service provider-accessible information stored on the access devices; and

preventing the end user from accessing the designated service provider-accessible information on the end user's access device.

11. (Original) The method as recited in claim 10, wherein the step of providing the control mechanism includes providing a software program for accessing and modifying the information of the access devices and designating portions thereof to prevent access by the end users.

12. (Original) The method as recited in claim 10, wherein the step of remotely accessing and modifying the end user network devices includes remotely accessing the end user devices from a service provider's location.

13. (Original) The method as recited in claim 10, wherein the information stored on the network access devices includes a configuration file for the access device.

14. (Original) The method as recited in claim 10, wherein the step of preventing the end user from accessing the designated information includes employing a security code for the designated portions to prevent access thereof by the end users.

15. (Original) The method as recited in claim 14, wherein the security code is associated with the designated portions at or before initializing the access devices.

16. (Original) The method as recited in claim 14, wherein the security code is associated with the designated portions after initializing the access devices.

17. (Original) The method as recited in claim 10, further comprising the step of assigning security for the stored information to prevent access thereof by the end users.

18. (Original) The method as recited in claim 17, wherein the security levels are associated with the designated portions at or before initializing the access devices.

19. (Original) The method as recited in claim 17, wherein the security levels are associated with the designated portions after initializing the access devices.

9. RELATED EVIDENCE APPENDIX

None.

10. RELATED PROCEEDINGS APPENDIX

None